



## הסכם סודיות ואבטחת מידע (עבור מחזיק במאגר מידע)

שנחתם ביום \_\_\_\_\_ לחודש \_\_\_\_\_ בשנת \_\_\_\_\_

בין

**אוניברסיטת בר אילן**

**ח.פ. 580063683**

(להלן: "האוניברסיטה")

לבין

ח.פ. \_\_\_\_\_

(להלן: "הספק")

והצדדים חתמו ביניהם על הסכם התקשרות ל- ביום XX/XX/XXXX	<b>הואיל</b>
;"ההסכם")	
ובמסגרת ההתקשרות הספק עשוי להיחשף למידע ממאגרי המידע של האוניברסיטה;	<b>והואיל</b>
והצדדים מעוניינים להסדיר את נושאי אבטחת המידע והגנת הפרטיות במסגרת השירותים בהתאם להוראות דיני הגנת הפרטיות.	<b>והואיל</b>

**לפיכך הוסכם, הוצהר והותנה בין הצדדים כדלקמן:**

### הוראות כלליות:

1. הספק מצהיר כי לשם מתן השירותים אשר פורטו בהסכם, הוא עשוי להיחשף למידע ממאגרי המידע ו/או למידע חסוי של האוניברסיטה, כמפורט להלן ("המידע המורשה"):
  - 1.1. [...]
  - 1.2. [...]וזאת למטרת ביצוע השירותים בלבד, כפי שהוגדרה בהסכם ("מטרת השירות");
2. העברת מידע בין הספק לאוניברסיטה או להיפך תתבצע באמצעות \_\_\_\_\_
3. במסגרת ההסכם, הספק אינו רשאי לגשת למערכות המידע / במסגרת ההסכם, הספק רשאי לגשת אך ורק למערכות המידע הבאות (מחק את המיותר):
  - 3.1. [...]
  - 3.2. [...]
4. הספק לא יעביר וכן לא יאפשר גישה ו/או הרשאות צפייה ו/או הרשאות עיבוד כלשהן לגבי המידע המורשה לאף גורם מבלי שקיבל את אישור האוניברסיטה מראש ובכתב. לשם כך, ולצורך ביצוע



השירותים המפורטים בהסכם בלבד, האוניברסיטה מאשרת לספק להתקשר עם ספקי המשנה הבאים:

- 4.1. [...] העברה אך ורק לצורכי \_\_\_\_\_.
- 4.2. [...]
- 4.3. [...]
5. הספק מצהיר בזאת כי בעת התקשרות עם ספק משנה כאמור בסעיף 4, יחתים הספק את ספק המשנה על הסכם התקשרות התואם באופן מהותי את הוראות הסכם זה. ביחס לספקי ענן גלובליים (כדוגמת AWS, AZURE, GCP) ניתן להסתפק בהסמכה לתקני אבטחה מקובלים, כדוגמת ISO27001 או SOC2 ו/או הצגת מדיניות פרטיות מתאימה, וזאת לאחר שהספק בחן את סיכוני אבטחת המידע הכרוכים בהתקשרות ומצא את ספק המשנה מתאים ובכפוף לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.
6. הספק מצהיר ומתחייב בזאת כי עם סיום ההתקשרות, מכל סיבה שהיא, ולכל היותר, בתום תקופת ההסכם, כל המידע המורשה שהגיע לרשותו במסגרת ההסכם יוחזר לרשות האוניברסיטה לפי בקשתו, ככל הניתן, יימחק מכל אמצעי המדיה שברשותו ו/או ברשות מי מטעמו. הספק יציג לאוניברסיטה תצהיר חתום על ידי מורשה החתימה של הספק המאמת ביצוע פעולות מחיקה, ביעור והשמדה כאמור.
7. הספק מתחייב לפעול על פי כל דין, לרבות הוראות חוק הגנת הפרטיות, תשמ"א-1981 (להלן: "החוק" או "חוק הגנת הפרטיות") התקנות שהותקנו לפיו, הנחיות רשם מאגרי המידע והרשות להגנת הפרטיות וכיוצא בזאת, ולפי הוראות שיתקבלו מעת לעת על ידי האוניברסיטה.
8. הספק לא יהא רשאי לעדכן ו/או להשיב לצדדים שלישיים בכל הנוגע למידע המורשה, ובכל מקרה בו נתקבל פנייה הנוגעת למידע המורשה המוחזק במערכות הספק, ינחה הספק את הפונה לפנות לאוניברסיטה (למעט אם קיימת חובה אחרת לפי כל דין).
9. הספק מתחייב לאפשר לאוניברסיטה ביצוע מעקב ובקרה שוטפים על קיום הוראות חוק הגנת הפרטיות והתקנות שהותקנו לפיו והוראות ההתקשרות וזאת על מנת לאפשר פיקוח על פעילותו של הספק בהתאם להוראות הדין. בכלל זאת, הספק מתחייב לאפשר לנציג האוניברסיטה לערוך ביקורת אבטחה בכל עת ובתיאום מראש.
10. הספק מתחייב להעביר דיווח מידי לאוניברסיטה בכל מקרה של חשש לדליפת המידע מהמאגר או שימוש חורג מההרשאה שניתנה לספק ו/או למי מטעמו.
11. הספק מתחייב לדווח לאוניברסיטה, אחת לשנה לפחות, על אופן ביצוע חובותיו לפי תקנות אבטחת מידע ולפי הסכם זה.
12. פרטי איש קשר מטעם הספק לצורך עדכון הספק כמחזיק במאגר המידע: שם מלא: \_\_\_\_\_; טלפון: \_\_\_\_\_; כתובת דוא"ל: \_\_\_\_\_.

### סודיות:

13. "מידע", במסמך זה: כל חומר, מסמך ו/או מידע אחר הנוגע לפעילות האוניברסיטה ו/או חבריה ו/או לקוחותיה ו/או עובדיה ו/או עסקיה אשר אינו נחלת כלל הציבור (למעט אם הפך לכה בשל מעשה/מחדל של הספק) לרבות, מבלי לגרוע מכלליות האמור לעיל, מידע אודות משאבי האוניברסיטה; מידע בדבר סודות מסחריים ו/או מקצועיים, הזמנות והסכמים מכל סוג ו/או מידע המוגן מכוח חוק הגנת הפרטיות ו/או בהתאם לכל דין אחר החל או עשוי לחול על האוניברסיטה.



14. ידוע לספק כי לצורך מתן השירותים לאוניברסיטה, תהא לו גישה למידע כהגדרתו לעיל. כמו כן, ידועה וברורה לספק רגישותו המיוחדת של המידע והצורך בשמירה קפדנית על חסיונו ועל הנזק הכבד שעשוי להיגרם עקב חשיפתו על ידי או עשיית שימוש בו על כל המשתמע מכך.
15. הספק מתחייב לשמור בסודיות מוחלטת כל מידע אשר יגיע אליו ו/או למי מטעמו מתוקף מתן השירותים לאוניברסיטה או בדרך אחרת. הספק מתחייב שלא להחזיק ברשותו ולא לעשות כל שימוש, בכל מידע באשר הוא שלא לצורכי ביצוע השירותים המפורטים בהסכם. הספק מתחייב שלא לגלות מידע כזה או חלקו, במישרין או בעקיפין, לכל אדם או גוף, אלא לצורך ביצוע השירותים לפי ההסכם ובכפוף להסכמת האוניברסיטה. למעט:
- 15.1. העברת מידע מוגבלת לעובדים (לרבות נותני שירות מטעם הספק) אשר להם צורך של ממש בקבלת המידע לצורך ביצוע השירותים בלבד, ובלבד שהובהר לעובדים אלה כי מדובר במידע סודי, והם חתומים כלפי הספק על כתב סודיות בנוסח דומה לכתב סודיות זה.
- 15.2. על פי דרישת ערכאה מוסמכת או רשות שלטונית מוסמכת על פי דין, ובלבד שהספק יודיע לאוניברסיטה באופן מידי על קבלת דרישה למסירת המידע (ככל שלא קיימת מניעה על פי דין למתן הודעה כאמור), ויאפשר לאוניברסיטה, ככל שהדבר בידי הספק, להתגונן בפני כל דרישה כאמור והספק ימסור רק את אותו חלק של המידע הסודי ו/או המידע החסוי שנדרש במפורש למסור.
16. הספק מתחייב לפעול כך שנתונים ומידע אשר יועברו אליו בהתאם להסכם זה, יאובטחו כך שלא תתאפשר גישה, בין באופן אקטיבי ובין באופן פאסיבי, למידע ולנתונים אלו, לאיש מלבד המורשים לכך החתומים על כתב התחייבות לשמירת סודיות כלפי האוניברסיטה.
17. הספק מתחייב שלא להעתיק ו/או להרשות לאחרים ו/או לגרום לאחר לבצע במידע – שכפול, העתקה, צילום, תדפיס וכל צורת העתקה אחרת שלא למטרת השירותים.
18. על העותקים של המידע יחולו הוראות התחייבות זו וכל האמור לגבי המידע יחול גם על עותקיו.
19. הספק מתחייב כי בכל מקרה שיתעוררו ספקות כלשהן בנוגע לתוכן התחייבויותיו לפי כתב התחייבות זה, וקיומו, יפנה לאוניברסיטה בכתב לקבלת אישורו. ידוע לספק כי אין בנאמר בפסקה זו לגרוע מכל התחייבות מהתחייבויותיו המנויות בכתב התחייבות זה.
20. למען הסר ספק, מוצהר ומוסכם כי אין בעצם גילוי המידע על ידי האוניברסיטה והעברתו אל הספק כדי להעניק לספק כל זכות במידע.
21. התחייבויות הספק דלעיל תחולנה עליו אישית וכן על כל תאגיד ו/או גוף שיקים ו/או שיהיה שותף בו, ו/או בעל שליטה בו, בין כבעל מניות, ובין בכל דרך אחרת, בין במישרין ובין בעקיפין, וכן על כל עובד מטעם הספק שייתן השירות.
22. תוקפה של התחייבות זו אינו מוגבל בזמן.
23. התחייבות זו לא תחול על מידע אשר התקבל מהאוניברסיטה ואשר הספק יוכיח לגביו בכתובים כי:
- 23.1. המידע היה ידוע לספק לפני קבלת המידע מהאוניברסיטה.
- 23.2. המידע היה ידוע ברבים או שהיה ניתן להשגה על ידי הציבור הרחב באופן חוקי לפני יום העברתו לספק.
- 23.3. המידע הפך למידע ציבורי או ניתן להשגה על ידי הציבור באופן חוקי לאחר מועד העברת המידע על ידי האוניברסיטה לספק בלא שהיה הוא אחראי או מעורב בתהליך.
- 23.4. המידע הגיע לספק בדרך חוקית של רכישת זכויות או בכל דרך חוקית שהיא.



24. ידוע ומוסכם כי האוניברסיטה תהא זכאית לפיצוי מהספק בגין כל נזק שייגרם בעקבות הפרה של איזו מהתחייבויותיו לפי כתב התחייבות זה, וזאת מבלי לפגוע בכל סעד אחר המוקנה לאוניברסיטה על פי דין ובלבד שהאוניברסיטה תודיע לספק על התביעה ו/או הדרישה ואפשר לו להתגונן כנגדה באופן עצמאי.

### **דרישות אבטחת מידע**

#### **25. הנחיות כלליות:**

- 25.1. בהתקיים חובה חוקית לפי התנאים המפורטים בסעיף 17 לחוק הגנת הפרטיות, הספק ימנה ממונה על אבטחת המידע (להלן: "הממונה"). הממונה יבטיח, בין היתר, שימוש נכון בזיהוי המשתמש ובסיסמא, בהרשאות הגישה למידע ובהגנת משאבי מערכות המחשב והמידע ומערכות התקשורת המכילות מידע השייך לאוניברסיטה. במידה שלא חלה חובה חוקית למינוי ממונה, הספק ימנה גורם מטעמו שיהיה אחראי לאבטחת המידע וסייבר.
- 25.2. הספק יגדיר נוהל אבטחת מידע, כמפורט בתקנה 4 לתקנות אבטחת המידע.
- 25.3. הספק יבצע סקר סיכונים ומבדק חדירה למאגרי מידע שחלה עליהם רמת אבטחה גבוהה, אחת ל-18 חודשים לכל הפחות.

#### **26. אבטחה פיסיית וסביבתית:**

- 26.1. הספק ישמור את מאגרי המידע וכן את התשתיות והמערכות המשמשות את המאגרים, במקום מוגן, המונע חדירה וכניסה אליו ללא הרשאה והתואם את אופי פעילות המאגר ורגישות המידע.
- 26.2. במאגרי מידע שחלה עליהם רמת אבטחה גבוהה/בינונית-הספק יבצע בקרה ותיעוד של הכניסה והיציאה מאתרים בהם מצויות מערכות המידע וכן בקרה ותיעוד של הכנסה והוצאת ציוד אל מערכות המאגר ומהן, וישמור תיעוד זה למשך 24 חודשים לכל הפחות.

#### **27. אבטחת מידע בניהול כוח אדם:**

- 27.1. הספק ייתן וישנה הרשאות גישה למידע המצוי במאגר המידע ומערכותיהם רק לאחר נקיטת אמצעים סבירים, המקובלים בהליכי מיון ושיבוץ עובדים.
- 27.2. הספק יקיים הדרכות לבעלי הרשאות גישה למידע מטעמו המצוי במאגרי המידע, בטרם מתן ההרשאות או בטרם שינוי ההרשאות הקיימות, וכן הדרכות תקופתיות ע"פ דרישות חוק הגנת הפרטיות והתקנות מכוחו. ההדרכות יעסקו בחובות לפי חוק הגנת הפרטיות, תקנות אבטחת המידע ומסירת מידע אודות חובות בעלי הרשאות לפי החוק ולפי נוהל האבטחה של הספק.

#### **28. הזדהות וניהול הרשאות:**

- 28.1. הספק יבצע בקרת הרשאות תקופתית לבעלי הרשאות מטעמו. במידה שהספק מפתח מערכת עבור האוניברסיטה, הספק יודא יכולת הפקה יזומה של דו"ח הרשאות תקפות עפ"י דרישת האוניברסיטה.
- 28.2. אופן זיהוי בעל הרשאה במחשבי הספק, המשמשים גישה למידע של האוניברסיטה ו/או מכילים מידע של האוניברסיטה, יעמוד בקריטריונים הבאים:
- 28.2.1. ככל הניתן, אופן הזיהוי ייעשה על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.



- 28.2.2. שימוש במדיניות סיסמאות חזקה המורכבת מאותיות וספרות, ובעלת אורך סיסמא מינימלי של 8 תווים.
- 28.2.3. החלפת סיסמאות לפחות כל 6 חודשים.
- 28.2.4. הגדרת מספר ניסיונות הקשה שגויים של סיסמא בטרם נעילת המשתמש (לכל היותר 5).
- 28.2.5. הגדרת Session Time Out לאחר פרק זמן של אי פעילות, המחייב זיהוי מחדש של המשתמש. ברירת המחדל לסיום Session תהיה 30 דקות (גם אם המערכת תנוהל מקומית).
- 28.2.6. הצפנת הסיסמאות בהצפנה חד כיוונית בבסיס הנתונים.
- 28.2.7. גישת אדמין (מנהל מערכת) תהיה באמצעות אימות רב שלבי (MFA).
- 28.2.8. יישום תיעוד לכל שינוי בטבלת ההרשאות.
- 28.2.9. הגדרת אופן טיפול בתקלות הקשורות באימות זהות.
- 28.3. ביטול הרשאות לבעל הרשאה שסיים את תפקידו ובמידת האפשר שינוי סיסמאות למאגר ולמערכות המאגר, שבעל הרשאה עשוי היה לדעת, תתבצע מיד עם סיום תפקידו של בעל ההרשאה.

### **29. בקרה ותיעוד גישה:**

- 29.1.1. הספק יתעד בלוג את השדות הבאים: זיהוי ואימות;
- 29.1.2. נעילות משתמש;
- 29.1.3. פעולות עדכון ע"י המשתמשים כולל שמירת ערך קודם;
- 29.1.4. העלאות תכנים;
- 29.1.5. גישה מרחוק;
- 29.1.6. תיעוד כל מקרה שבו התגלה אירוע אבטחת מידע. ככל האפשר יבוסס התיעוד על רישום אוטומטי.
- 29.2. הספק ישמור את הלוגים הנ"ל באופן מאובטח, למשך 24 חודשים, לכל הפחות.
- 29.3. הספק יגדיר נוהל בדיקה שגרתית של הלוגים למנגנון הבקרה כולל דו"ח של הבעיות שהתגלו והצעדים שנקטו בעקבותיהן.

### **30. אירועי אבטחת מידע:**

- 30.1. הספק יגדיר הוראות בנוהל האבטחה שלו לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן הוראות לעניין דיווח למנהל אבטחת המידע של האוניברסיטה על אירועי אבטחה ועל הפעולות שנקטו בעקבותיהם.

### **31. ניהול מאובטח ומעודכן:**

- 31.1. הספק יגביל / ימנע אפשרות חיבור התקנים ניידים וינקוט אמצעי הגנה.
- 31.2. הספק יתקין תוכנת הגנה תקנית ומעודכנת נגד נזקות על מחשבים המכילים מידע השייך לאוניברסיטה.
- 31.3. הספק יישם בקרות קלט ופלט.
- 31.4. הספק יפריד, ככל הניתן, בין המערכות אשר ניתן לגשת מהן למידע שבמאגר, לבין מערכות מחשוב אחרות שמשמשות את הספק.
- 31.5. הספק יבצע הפרדה בין הנתונים של האוניברסיטה לבין נתונים של לקוחות אחרים. הפרדה כאמור יכולה להיות לוגית, תוך מתן הסבר לאוניברסיטה על אופן הפרדה.
- 31.6. הספק יישם הגנות על בסיס הנתונים והקשחות עפ"י הנחיות היצרן.



- 31.7. הספק יוודא ניטור שינויים בבסיסי הנתונים והפקת דו"ח למנהל אבטחת המידע של האוניברסיטה לפי דרישתו.
- 31.8. זמינות מרבית – הספק ידווח לאיש הקשר באוניברסיטה על כל השבתה של המערכת.
- 31.9. הספק ישמור את המידע כל עוד נמשך השירות.
- 31.10. הספק יוודא שימוש במערכות הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה בגרסאות נתמכות בלבד. לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.

### 32. אבטחת תקשורת וסביבת הפעלה:

- 32.1. הספק ינקוט באמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין האוניברסיטה אל הספק (לכל הפחות - Firewall ו-IPS, הצפנה בפרוטוקול TLS 1.2 ומעלה).
- 32.2. הספק לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, ללא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש.
- 32.3. בגישה מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, הספק יעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה שמטרת לזהות את המתקשר והמאמת את הרשאתו לביצוע הפעילות מרחוק ואת היקפה (לדוגמה: OTP, גישה מכתובת IP קבועה, Token, וכיו"ב).

### 33. גיבויים ושחזורים:

הספק יגדיר נוהל לביצוע גיבויים ושחזורים של נתוני האבטחה, בהתאם לתקנות 17 ו-18 לתקנות אבטחת מידע.

### 34. דרישות נוספות במקרה של פעילות בענן-

**יש להתאים סעיף זה לתכולת השירות בענן - IaaS/PaaS/SaaS** תוך התייחסות לנושאים הבאים:

- 34.1. אמנת שירות להבטחת זמינות המידע (SLA) - הספק מתחייב למתן מענה מיטבי והולם תוך        שעות, במקרה של אירוע אבטחת מידע. כך שזמן החזרה לכשירות וזמינות המידע יהיה בצורה המהירה ביותר.
- 34.2. במידה ומיקומה הגיאוגרפי של פעילות הענן הינה מחוץ לגבולות מדינת ישראל, הנ"ל יתבצע תוך עמידה בתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001, וכן כל תקן ו/או רגולציה נדרשת אחרת.
- 34.3. הספק יבצע תהליך ניהול פגיעויות מתמשך, זאת באמצעות כלי סריקה אוטומטיים. את תוצאות הסריקה על הספק לדרג ע"פ רמות חומרה, תוך טיפול באופן מידי בממצאים ברמת חומרה גבוהה וביסוס תוכנית עבודה מתאימה לטיפול בשאר הפגיעויות שנמצאו.
- 34.4. במידת הצורך, ולצורך מתן מענה אבטחתי עבור פגיעויות אבטחה שנמצאו בסריקת מערכות המידע שבהחזקת הספק-האחרון יבצע התאמות טכנולוגיות נדרשות, הכוללות בין היתר התקנת עדכוני יצרן מתאימים.
- 34.5. לצורך מתן מענה לאתגרי וסיכוני "נעילה" (Vendor lock-in) במסגרת חברת שירותי הענן הקיימת, יתבצע תיעוד כלל הממשקים וה-API אשר נעשה בהם שימוש, וכן גיבוי תקופתי של המידע הקיים בסביבת הענן לסביבת צד ג' אחרת. האמור מתייחס גם ל-Meta Data הרלוונטי.



- 34.6. תבצע החלפה תקופתית של מפתחות ההצפנה, ובפרט של API&Host keys, זאת לצורך שמירה על סודיות, שלמות ואמינות המידע.
- 34.7. במידת הצורך ועבור מתן מענה ראוי לאתגרי וסיכוני אבטחה רלוונטיים, הספק יבצע שימוש בטכנולוגיות הצפנה נוספות, כדוגמת-Masking , Anonymization וכן Tokenization.

**ולראיה באתי על החתום :**

שם + שם משפחה \_\_\_\_\_ תפקיד \_\_\_\_\_

תאריך \_\_\_\_\_ חתימה + חותמת \_\_\_\_\_